(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000357127 A**

(43) Date of publication of application: **26.12.00**

(51) Int. Cl **G06F 12/14**

(21) Application number: **11170189**

(22) Date of filing: **16.06.99**

(71) Applicant: **TOSHIBA CORP**

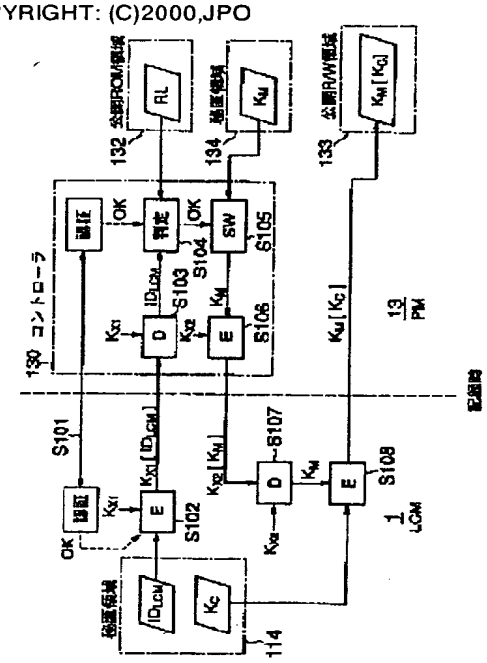
(72) Inventor: **KAMIBAYASHI TATSU**
YAMADA HISASHI
IWASAKI HIROSHI
TAMURA MASABUMI
ISHIBASHI YASUHIRO
KATO HIROSHI
TOMA HIDEYUKI

(54) **STORAGE MEDIUM AND COSNTENTS MANAGING METHOD USING THE MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To surely detect and make ineffective a device which has a problem and to use discrimination information characteristic of an unusable storage medium to cipher or decipher contents or a contents key when a device which is not made ineffective is made ineffective.

SOLUTION: In an open ROM area 132 secured on a PM (storage medium) 13, a revocation list RL is previously registered and when the PM 13 is used to record contents by, for example, an LCM (contents use management system) 1, a controller 130 of the PM 13 receives discrimination information IDLCM (ciphered information of which) of the LCM 1, refers to the list RL according to the information, and decides whether or not the LCM 1 is made ineffective according to the reference result. Only when it is decided that the LCM is not made ineffective, a media key KM made secret in a secret area 134 is (ciphered and) passed to the LCM 1 and used to cipher the contents key KC.



(19) 日本国特許庁 (JP)

(12) 公開特許公報（A）

(11) 特許出願公開番号

特開２０００－３５７１２７
(P２０００－３５７１２７A)
(43) 公開日 平成12年12月26日(2000.12.26)

(51)Int.Cl.[7]	識別記号	FI			テーマコード(参考)
G06F 12/14	320	G06F	12/14	320 F	5B017
				320 B	

審査請求 未請求 請求項の数 １０ ＯＬ （全 １４ 頁）

(21) 出願番号 特願平11-170189

(22) 出願日 平成11年6月16日(1999.6.16)

(71) 出願人 000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72) 発明者 上林 達
神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 山田 尚志
東京都港区芝浦一丁目1番1号 株式会社東芝本社事務所内

(74) 代理人 100058479
弁理士 鈴江 武彦 (外6名)

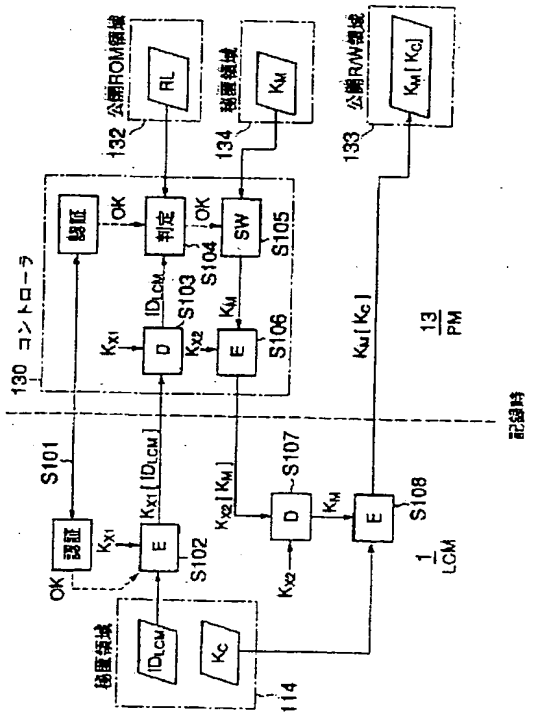
最終頁に続く

(54)【発明の名称】記憶媒体及び同媒体を使用したコンテンツ管理方法

(57)【要約】

【課題】問題のある機器を確実に検出して無効化し、無効化しない機器の場合、無効化されたならば利用不可能な記憶媒体に固有の識別情報をコンテンツまたはコンテンツキーの暗号化または復号化に用いさせることができるようにする。

【解決手段】ＰＭ（記憶媒体）１３上に確保された公開ＲＯＭ領域１３２に、リボケーションリストＲＬを予め登録しておき、当該ＰＭ１３が例えばＬＣＭ（コンテンツ利用管理システム）１によるコンテンツの記録に用いられる場合に、ＰＭ１３のコントローラ１３０が、ＬＣＭ１の識別情報ID_{LCM}（の暗号化情報）を受け取って、その情報によりリストＲＬを参照し、その参照結果に応じてＬＣＭ１を無効化するか否かを判定する（ステップＳ１０４）。そして、無効化しないと判定した場合だけ、秘匿領域１３４に秘匿されているメディアキーK_Mを（暗号化して）ＬＣＭ１に渡して、コンテンツキーK_Cの暗号化に用いさせる。



1

【特許請求の範囲】

【請求項１】　デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、

コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された特定記憶領域と、

任意の電子機器による記録または再生に利用される場合に、当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記リボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定する判定手段と、前記判定手段により無効化すべきでないと判定された場合だけ、前記電子機器に対して自身に固有の秘匿されたメディア識別情報を渡して、そのメディア識別情報をコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化に用いさせる暗号化／復号化キー送出手段とを含むコントローラとを具備することを特徴とする記憶媒体。

【請求項２】　デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、

コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が記憶される特定記憶領域と、

リボケーション情報が付加されたデジタルコンテンツが電子機器により記録される際に、当該リボケーション情報により前記特定記憶領域上のリボケーション情報を更新する更新手段と、デジタルコンテンツが電子機器により記録される際と、前記記憶媒体に記録されたデジタルコンテンツが電子機器により利用される際には、当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記特定記憶領域に記憶されているリボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、その判定結果に応じて当該電子機器の無効化を制御する判定手段とを含むコントローラとを具備することを特徴とする記憶媒体。

【請求項３】　デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、

コンテンツ保護のために無効化すべき電子機器が判別可能なバージョン情報付きリボケーション情報が記憶される特定記憶領域と、

バージョン情報付きリボケーション情報が付加されたデジタルコンテンツが電子機器により記録される際に、当該リボケーション情報のバージョン情報と前記特定記憶領域に記憶されているリボケーション情報のバージョン情報とを比較し、その比較結果に基づいて前記特定記憶

2

領域に最新のリボケーション情報が記憶されるように更新制御する更新手段と、デジタルコンテンツが電子機器により記録される際と、前記記憶媒体に記録されたデジタルコンテンツが電子機器により利用される際には、当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記特定記憶領域に記憶されているリボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、その判定結果に応じて当該電子機器の無効化を制御する判定手段とを含むコントローラとを具備することを特徴とする記憶媒体。

【請求項４】　デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、

コンテンツ保護のために無効化すべき電子機器が判別可能なバージョン情報付きリボケーション情報が記憶される特定記憶領域と、

バージョン情報付きリボケーション情報が付加された暗号化デジタルコンテンツであって、当該リボケーション情報が前記コンテンツを復号するためのコンテンツキーと合わせてシステムに共通のマスタキーにより暗号化された暗号化デジタルコンテンツが電子機器により記録される際に、当該リボケーション情報のバージョン情報と前記特定記憶領域に記憶されているリボケーション情報のバージョン情報とを比較し、その比較結果に基づいて前記特定記憶領域に最新のリボケーション情報が記憶されるように更新制御する更新手段と、暗号化デジタルコンテンツが電子機器により記録される際と、前記記憶媒体に記録された暗号化デジタルコンテンツが電子機器により利用される際には、当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記特定記憶領域に記憶されているリボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、その判定結果に応じて当該電子機器の無効化を制御する判定手段と、前記記憶媒体に記録された暗号化デジタルコンテンツが電子機器により利用される際は、前記判定手段により無効化すべきでないと判定された場合だけ、当該電子機器に対して秘匿された前記マスタキーを渡して、そのマスタキーをコンテンツ復号用のコンテンツキーの復号化に用いさせるマスタキー送出手段とを含むコントローラとを具備することを特徴とする記憶媒体。

【請求項５】　デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶メディア部とコントローラとが一体化された記憶媒体に特定記憶領域を設けて、当該特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報を予め登録しておき、

前記記憶媒体の１つが任意の電子機器による記録または再生に利用される場合に、その記憶媒体上の前記コントローラにて当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記リボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、

無効化すべきでないと判定した場合だけ、前記記憶媒体上のコントローラから前記電子機器に対して当該記憶媒体に固有の秘匿されたメディア識別情報を渡し、

前記電子機器では前記メディア識別情報をコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化に用いることを特徴とするコンテンツ管理方法。

【請求項６】　前記記憶媒体のコントローラと前記電子機器との間で、前記電子機器を表す情報、前記メディア識別情報の授受を行う際には、その都度前記コントローラと前記電子機器との間で所定のアルゴリズムに従うキー交換を行って認証鍵を共有し、前記電子機器を表す情報、前記メディア識別情報の送り側では、当該情報を自身の有する前記認証鍵で暗号化して送り、受け側では、暗号化された情報を自身の有する前記認証鍵で復号して使用することを特徴とする請求項５記載のコンテンツ管理方法。

【請求項７】　配信する暗号化デジタルコンテンツ、または記憶媒体に記録された暗号化デジタルコンテンツに、コンテンツ保護のために無効化すべき、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器が判別可能なリボケーション情報を付加し、

前記暗号化デジタルコンテンツを、記憶メディア部とコントローラとが一体化された記憶媒体に電子機器により記録する際には、その記憶媒体上の前記コントローラにて当該電子機器から当該電子機器を表す情報と前記リボケーション情報が付加された暗号化デジタルコンテンツを受け取って、その受け取った電子機器を表す情報により前記リボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、

無効化すべきでないと判定した場合だけ前記暗号化デジタルコンテンツを前記記憶媒体に記録することを特徴とするコンテンツ管理方法。

【請求項８】　前記リボケーション情報に予めバージョン情報を付す一方、最新のリボケーション情報を前記記憶媒体の特定記憶領域に記憶せしめ、

前記暗号化デジタルコンテンツを、前記記憶媒体に前記電子機器により記録する際には、当該コンテンツに付加されているリボケーション情報のバージョン情報と、前記特定記憶領域に記憶されているリボケーション情報のバージョン情報とを比較して、その比較結果に基づいて最新のリボケーション情報が前記特定記憶領域に記憶されるように制御し、

前記特定記憶領域に記憶されている最新のリボケーション情報を用いて前記電子機器を無効化すべきか否かの判定を行うことを特徴とする請求項７記載のコンテンツ管理方法。

【請求項９】　前記暗号化デジタルコンテンツに付加される前記リボケーション情報は、当該コンテンツを復号するためのコンテンツキーと合わせて、システムに共通のマスタキーにより暗号化されており、

前記記憶媒体に記録された暗号化デジタルコンテンツを電子機器により利用する際には、その記憶媒体上の前記コントローラにて当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記特定領域に記憶されているリボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、

無効化すべきでないと判定した場合だけ、前記記憶媒体上のコントローラから前記電子機器に対して秘匿された前記マスタキーを渡し、

前記電子機器では前記マスタキーを前記コンテンツキーの復号化に用いることを特徴とする請求項７記載のコンテンツ管理方法。

【請求項１０】　コンテンツ保護のために無効化すべき、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器が判別可能なリボケーション情報が予め登録された特定記憶領域を有する記憶メディア部とコントローラとが一体化された記憶媒体とのインタフェースを持ち、当該インタフェースを通してコンテンツの記録または再生が可能な電子機器であって、

前記記憶媒体をデジタルコンテンツの記録または再生に利用するに際し、自身を表す情報を前記記憶媒体に渡すことで、当該情報により前記記憶媒体のコントローラにて前記リボケーション情報を参照させて、その参照結果に応じて前記記憶媒体に固有の秘匿されたメディア識別情報を前記コントローラから受け取る手段と、

前記メディア識別情報によりコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化を行う手段とを具備することを特徴とする電子機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、画像データや音楽データに代表される種々のデジタルコンテンツを記録再生するのに用いられる記憶媒体に係り、特に不当な電子機器によるコンテンツの記録再生を抑止するのに好適な記憶媒体及び同媒体を使用したコンテンツ管理方法に関する

【０００２】

【従来の技術】近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレーヤー、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メデ

ィアに格納された画像データや音楽データなど様々なデジタルコンテンツを再生できるほか、インターネット等を通じてデジタルコンテンツをダウンロードして使用することもできる。

【０００３】これらのデジタルコンテンツは、例えばＭＰＥＧ２、ＭＰ３といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用から保護するための技術の必要性が叫ばれている。

【０００４】

【発明が解決しようとする課題】しかし、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器で用いられる記憶媒体は、別の機器に移動しても記録／再生できるリバーシブルなものが多く、その仕様は基本的にはオープンである。このためコンテンツの移動／コピーを自由に行うことができるので、記憶媒体に記憶されたコンテンツを不正なコピー／移動から保護することは実際上困難である。

【０００５】そこで、メモリカードのように記憶メディア部とコントローラとが一体化された記憶媒体については、秘匿された特定手続にてのみアクセスでき、ユーザからはアクセスできないアクセス不能領域（秘匿領域）を設け、そこにコピー制御情報、移動制御情報などの、コンテンツの使用に必要な重要な情報を格納しておくことにより、コンテンツの保護を図ることが考えられる。

【０００６】この場合、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器と記憶媒体の間でコンテンツのコピー／移動を行う際には、それぞれが、著作権保護（コンテンツ保護）に関する所定の仕組み（つまり所定のコンテンツ保護機能）を共有している正当なものであるかを相互に認証し、正しいと認証できた場合に相互に共有する鍵生成のアルゴリズムに従って鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキー（コンテンツを暗号化するキー）の暗号化（ライセンス暗号化）／復号化またはコンテンツの暗号化／復号化に用いることも考えられる。

【０００７】ところが、上記相互認証に必要な情報は、機器の出荷段階で予め設定されていることから、機器の購入後に当該機器（上で動作するプログラム）が改変されるといった攻撃により、例えばコンテンツ保護の仕組みが無用なものになった場合等においては、上記相互認証だけでは、この種の、問題のある機器を検出できないことになる。

【０００８】しかも、上記した問題のある機器を検出する方法が考えられたとしても、相互に鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキーの暗号化／復号化またはコンテンツの暗号化／復号化に用いる方式では、この種の機器を排除できないことが予測される。その理由は、たとえ問題のある機器が検出

できたとしても、その機器と記憶媒体との間で認証鍵の交換が行われると、その認識鍵を用いてコンテンツキーの暗号化／復号化またはコンテンツの暗号化／復号化が行われるからである。

【０００９】本発明は上記事情を考慮してなされたものでその目的は、無効化すべき電子機器が判別可能なリボケーション情報に基づいて問題のある機器を確実に検出して無効化すると共に、無効化しない機器の場合には、無効化されたならば利用不可能な記憶媒体に固有の識別情報をコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化に用いさせることで、不当な機器による利用を確実に防止できる記憶媒体及び同媒体を使用したコンテンツ管理方法を提供することにある。

【００１０】本発明の他の目的は、リボケーション情報を常に最新なものに更新できる記憶媒体及び同媒体を使用したコンテンツ管理方法を提供することにある。

【００１１】

【課題を解決するための手段】本発明の記憶媒体は、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された特定記憶領域と、任意の電子機器による記録または再生に利用される場合に、当該電子機器から当該電子機器を表す情報を受け取って、その情報により上記リボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定する判定手段と、この判定手段により無効化すべきでないと判定された場合だけ、上記電子機器に対して自身に固有の秘匿されたメディア識別情報を渡して、そのメディア識別情報をコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化に用いさせる暗号化／復号化キー送出手段とを含むコントローラとを備えたことを特徴とする。

【００１２】このように本発明の記憶媒体においては、その特定記憶領域にリボケーション情報が予め登録された構成とする一方、メモリカードのように、記憶メディア部とコントローラとが一体化された構成とし、当該記憶媒体が任意の電子機器による記録または再生に利用される場合に、上記コントローラが当該電子機器から当該電子機器を表す情報を受け取って、その情報によりリボケーション情報を参照し、その参照結果に応じて当該電子機器の無効化を制御すると共に、無効化すべきでない場合には、電子機器に対して自身に固有の秘匿されたメディア識別情報を渡して、そのメディア識別情報をコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化に用いさせることにより、リボケーション情報から正当と認められる電子機器においてのみ、コンテンツまたはコンテンツキーの暗号化／復号化が可能となり、記憶媒体側で不当な電子機器によるコンテンツ

の記録または再生を確実に抑止することが可能となる。

【００１３】ここで、上記特定記憶領域を、読み出し専用の不揮発性メモリ上に確保するか、或いは秘匿された特定手続以外ではアクセスできない書き換え可能な不揮発性メモリ上に確保するならば、リボケーション情報の改ざんにも対処可能となる。

【００１４】また、本発明の記憶媒体は、リボケーション情報が付加されたデジタルコンテンツを扱う新規なシステムに対応可能なように、上記コントローラとして、以下の各手段、即ちリボケーション情報が付加されたデジタルコンテンツが電子機器により記録される際には、当該リボケーション情報により上記特定記憶領域上のリボケーション情報を更新する更新手段と、デジタルコンテンツが電子機器により記録される際と、本記憶媒体に記録されたデジタルコンテンツが電子機器により利用される際には、当該電子機器から当該電子機器を表す情報を受け取って、その情報により上記特定記憶領域に記憶されている最新のリボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、その判定結果に応じて当該電子機器の無効化を制御する判定手段とを備えたコントローラを用いたことをも特徴とする。ここで、上記特定記憶領域を、秘匿された特定手続以外ではアクセスできない書き換え可能な不揮発性メモリ上に確保するとよい。

【００１５】このような構成の記憶媒体とすることで、当該記憶媒体の特定記憶領域に登録されるリボケーション情報を常に最新のものに更新することができ、不当な電子機器によるコンテンツの記録（コピー）を効果的に防止することができる。

【００１６】また、デジタルコンテンツに付加されるリボケーション情報にバージョン情報が付されるシステム、即ちバージョン情報付きリボケーション情報（バージョン管理されたリボケーション情報）を扱うシステムに対処可能なように、上記更新手段に、デジタルコンテンツに付加されたリボケーション情報のバージョン情報と上記特定記憶領域に記憶されているリボケーション情報のバージョン情報とを比較し、その比較結果に基づいて上記特定記憶領域に最新のリボケーション情報が記憶されるように更新制御する機能を持たせるならば、上記バージョン情報を有効利用して、記憶媒体の特定記憶領域に登録されるリボケーション情報を確実に最新のものに更新することができる。

【００１７】また、本発明の記憶媒体は、バージョン情報付きリボケーション情報が付加された暗号化デジタルコンテンツであって、当該リボケーション情報がコンテンツ復号用のコンテンツキーと合わせてシステムに共通のマスタキーにより暗号化された暗号化デジタルコンテンツを扱う新規なシステムに対応可能なように、上記コントローラに次の手段、即ち上記判定手段により無効化すべきでないと判定された場合だけ、該当する電子機器

に対して秘匿されたマスタキーを渡して、そのマスタキーをコンテンツ復号用のコンテンツキーの復号化に用いさせるマスタキー送出手段を設けたことをも特徴とする。この構成においては、不当な電子機器によるコンテンツの利用（例えば再生）を効果的に防止することができる。

【００１８】なお本発明は、上記構成の記憶媒体を使用したコンテンツ管理方法としても成立し、上記構成の記憶媒体を利用する、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器としても成立する。

【００１９】

【発明の実施の形態】以下、本発明の実施の形態につき図面を参照して説明する。

【００２０】図１は本発明の一実施形態に係るコンテンツ利用管理システム１の構成例を示す。なお、ここでは、コンテンツ（デジタルコンテンツ）として音楽データを一例として用いているが、この場合に限らず、映画や、ゲームソフト等のデータであってもよい。

【００２１】ＥＭＤ（Electronic Music Distributor）は、音楽配信サーバまたは音楽配信放送局である。

【００２２】コンテンツ利用管理システム（以下、ＬＣＭ（Licence (SDMI-)Compliant Module）と称する）１は、例えば、パーソナルコンピュータ（ＰＣ）を用いて実現される。このＬＣＭ１におけるコンテンツ保護の方法は、コンテンツを記録すべき記憶メディア（記憶媒体）１３毎に、その記憶メディアの識別情報（メディアＩＤ）を用いてコンテンツの暗号化／復号化を管理することを前提としている。

【００２３】ＬＣＭ１は、複数のＥＭＤ（ここでは、ＥＭＤ＃１～＃３）に対応した受信部＃１～＃３を有しており、当該受信部＃１～＃３を通してＥＭＤが配信する暗号化コンテンツまたはそのライセンス（利用条件と暗号化コンテンツ復号キー）などを受信する。受信部＃１～＃３は、再生機能や課金機能を有していても良い。また、課金機能を利用して、気に入ったコンテンツを購入することが可能である。

【００２４】ＬＣＭ１は、セキュア・コンテンツ・サーバ（ここでは、Secure Music Server：ＳＭＳであり、以下ＳＭＳと称する）２を有する。このＳＭＳ２は、利用者が購入した暗号化コンテンツをＥＭＤＩ／Ｆ（インタフェース）部３を経由して受け取る。暗号化コンテンツ（ここでは音楽コンテンツ）は、必要に応じてＥＭＤＩ／Ｆ部３で復号され、形式変換や再暗号化が施される。ＳＭＳ２は暗号化コンテンツを受け取ると、それを音楽データ格納部１０に格納し、音楽データ復号鍵（コンテンツ復号キー）をライセンス格納部９に格納する。ここでＳＭＳ２は、配信された音楽コンテンツを利用者が試聴するために再生機能を有していても良く、この場合、ＳＭＳ２が管理する音楽コンテンツをＰＣ上で再生

することができる。

【００２５】ＳＭＳ２はまた、メディアＩ／Ｆ部６に装着可能なメモリカード等の記憶メディア（以下、ＰＭ（Portable Memory）と称する）１３に対してコンテンツデータ（デジタルコンテンツ）を当該Ｉ／Ｆ部６経由で出力する機能を有している。このＰＭ１３は、図２に示す構成の専用の記録再生装置（以下、簡単にＰＤ（Portable Device）と称する）１２にセットして用いることで、当該ＰＭ１３に記録されたコンテンツをＰＤ１２上で再生することができる。

【００２６】ＳＭＳ２からＰＭ１３へのコンテンツの記録は、メディアＩ／Ｆ部６を通じて直接行われるか、またはＰＤ１２を経由して行うことができる。

【００２７】ここで、ＬＣＭ１によるチェックイン／チェックアウト機能について簡単に説明する。チェックアウトとは、ＬＭＳ１が「親」としてのコンテンツを格納しており、ＰＭ１３に、その複製を「子」コンテンツとしてコピーすることをいう。「子」コンテンツは基本的にはＰＤ１２で自由に再生することが可能であるが、「子」から「孫」コンテンツを作成することは許されない。「親」が幾つ「子」を生むことができるかは、「親」の属性として定義される。また、チェックインとは、例えば、ＰＭ１３をＬＣＭ１のメディアＩ／Ｆ部６に装着し、ＬＣＭ１が「子」コンテンツを消去（または利用不能）することで、ＬＣＭ１内の「親」コンテンツは「子」を１つ作る権利を回復することをいう。これを「親」にチェックインするともいう。

【００２８】ＰＭ１３は、図３に示すように、コントローラ１３０と、公開領域１３１及び秘匿領域１３４からなる記憶メディア部とから構成される。秘匿領域１３４は、コントローラ１３０を通して非公開の手順（つまり秘匿された特定手続）でしかアクセスできない記憶領域であり、コンテンツ復号に必要な情報を記憶するのに用いられる。秘匿領域１３４は、対応するＰＭ１３に固有のメディア識別情報（以下、メディアキーと称する）K_M等の定数が記憶される秘匿ＲＯＭ領域と、ライセンスする側から提供される（メディアマークと呼ばれる）秘密データであるライセンス復号キー等の変数が記憶される秘匿Ｒ／Ｗ（リード／ライト）領域からなる。メディアキーK_Mは、各ＰＭ１３に固有であればよく、シリアル番号や製造番号（ＰＭ１３個々の製造番号、または製造ロット番号）、他の様々な識別情報を用いることができる。なお、メディアキーK_Mを、各ＰＭ１３に固有な識別情報とライセンス復号キーから生成するようにしても構わない。秘匿ＲＯＭ領域は例えばＲＯＭ（読み出し専用の不揮発性メモリ）上に確保され、秘匿Ｒ／Ｗ領域は例えばフラッシュメモリ（書き換え可能な不揮発性メモリ）の特定領域に確保される。

【００２９】公開領域１３１は、秘匿領域以外の、通常の手順にてアクセス可能な領域であり、読み出し専用の公開領域（以下、公開ＲＯＭ領域と称する）１３２と、書き換え可能な公開領域（以下、公開Ｒ／Ｗ領域と称する）１３３からなる。公開ＲＯＭ領域は例えばＲＯＭ上に確保され、公開Ｒ／Ｗ領域は例えばフラッシュメモリ上に確保される。この公開ＲＯＭ領域、公開Ｒ／Ｗ領域は、先の秘匿ＲＯＭ領域が確保されるＲＯＭ、秘匿Ｒ／Ｗ領域が確保されるフラッシュメモリ上に、それぞれ確保されるようにしても構わない。

【００３０】公開ＲＯＭ領域１３２には、本発明に直接関係するリボケーション情報が対応するＰＭ１３の出荷段階で予め登録されている。このリボケーション情報は、コンテンツの保護のためにＰＭ１３の利用を無効化すべき機器（ＬＣＭ，ＰＤ）、更に具体的に述べるならばＰＭ１３（内の公開Ｒ／Ｗ領域１３３）を対象とするデジタルコンテンツの記録または再生のためのアクセス要求を無効化すべき機器（ＬＣＭ、ＰＤ）が判別可能な情報である。本実施形態において、リボケーション情報は無効化すべき機器の識別情報（デバイスＩＤ）のリストである。そこで、以下の説明では、「リボケーション情報」に代えて「リボケーションリストＲＬ」なる用語を用いる。つまり、公開ＲＯＭ領域１３２には、リボケーションリストＲＬが予め登録されている。

【００３１】公開Ｒ／Ｗ領域１３３には、暗号化されたコンテンツキー（コンテンツ復号キー）、暗号化されたコンテンツ等が適宜記憶される。暗号化されたコンテンツキーは、コンテンツＣを復号するための（当該コンテンツＣに固有の）コンテンツキーK_Cを、ＰＭ１３に依存するメディアキーK_Mで暗号化することで取得されるものである。また、暗号化されたコンテンツ（ここでは２重に暗号化されたコンテンツ）は、K_Cで暗号化されたコンテンツ（K_C［Ｃ］）をＰＭ１３に依存するメディアキーK_Mで暗号化する（K_M［K_C［Ｃ］］）ことで取得されるものである。

【００３２】ＬＣＭ１、ＰＤ１２もまた、図４に示すようにＰＭ１３と同様の記憶領域を有している。即ちＬＣＭ１は、公開ＲＯＭ領域１１２及び公開Ｒ／Ｗ領域１１３からなる公開領域１１１と、非公開の手順でしかアクセスできない秘匿領域１１４との各記憶領域を有している。公開Ｒ／Ｗ領域１１３には、図１に示す音楽データ格納部１０が確保されている。秘匿領域１１４には、ＬＣＭ１の識別情報（デバイスＩＤ）ID_{LCM}が予め記憶されている。秘匿領域１１４にはまた、各コンテンツ毎のコンテンツキーK_Cが適宜記憶される。秘匿領域１１４には更に、図１に示す宿帳格納部８が確保されている。ＳＭＳ２の管理下にある音楽データ格納部１０（公開Ｒ／Ｗ領域１１３）にて保持される全ての音楽コンテンツは、その識別情報であるコンテンツＩＤ（ＴＩＤ）と予め定められた複製可能コンテンツ数、即ち子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼び、（秘匿領域１１４内の）宿

帳格納部８に格納される。ＬＣＭ１は、ＳＭＳ２にてこの宿帳格納部８にアクセスするための秘匿された特定の手続が行われた後、宿帳格納部８（を提供する秘匿領域１１４）からデータを読み取るための秘匿領域ドライバ７を有している。なお、この宿帳は本発明に直接関係しないため、その利用方法の詳細については説明を省略する。

【００３３】一方、ＰＤ１２は、公開ＲＯＭ領域１２２及び公開Ｒ／Ｗ領域１２３からなる公開領域１２１と、非公開の手順でしかアクセスできない秘匿領域１２４との各記憶領域を有している。秘匿領域１２４には、ＰＤ１２の識別情報$ＩＤ_{PD}$が予め固定記憶されている。秘匿領域１２４にはまた、各コンテンツ毎のコンテンツキーK_Cが適宜記憶される。

【００３４】図２は、ＰＤ１２の構成例を示す。ＰＭ１３は、ＰＤ１２のメディアＩ／Ｆ部１２ｆに装着して利用される。ＬＣＭ１がＰＤ１２を介してＰＭ１３に読み書きする場合は、ＬＣＭ１内のＰＤＩ／Ｆ部５、ＰＤ１２内のＬＣＭ-Ｉ／Ｆ部１２ｅ、メディアＩ／Ｆ部１２ｆを経由して当該ＰＭ１３の秘匿領域１３４（図３参照）にアクセスする。メディアＩ／Ｆ部１２ｆは、ＰＭ１３の秘匿領域１３４にアクセスするための秘匿領域アクセス部（図示せず）を有している。ＰＤ１２内の公開Ｒ／Ｗ領域１２３及び秘匿領域１２４（図４参照）は、例えばフラッシュメモリ１２ｄ上に確保されている。また公開ＲＯＭ領域１２２（図４参照）は、ＲＯＭ１２ｃ上に確保されている。このＲＯＭ１２ｃには、ＰＭ１３との間で相互認証を行うためのプログラムが書き込まれている。ＰＤ１２では、ＣＰＵ１２ａの制御のもと、このプログラムに従ってＰＭ１３との間の相互認証等の処理が実行される。

【００３５】次に、本実施形態の動作について、ＥＭＤから配信された暗号化された音楽コンテンツをＬＣＭ１のＥＭＤＩ／Ｆ部３で受信して、ＳＭＳ２により音楽データ格納部１０に一時格納した後、その「複製」を「子」コンテンツとして、例えばメディアＩ／Ｆ部６に装着されたＰＭ１３に記録（コピー）するチェックアウト時の動作を例に、図５の流れ図を参照して説明する。

【００３６】この場合、チェックアウトの指示が例えばＬＣＭ１のユーザＩ／Ｆ部１５を介してなされ、且つＰＭ１３がＬＣＭ１のメディアＩ／Ｆ部６に装着された段階で、ＬＣＭ１のメディアＩ／Ｆ部６とＰＭ１３のコントローラ１３０との間で周知の相互認証が行われる（ステップＳ１０１）。この相互認証は、ＬＣＭ１を機器Ａ、ＰＭ１３を機器Ｂとすると、次のように行われるのが一般的である。

【００３７】まず、機器Ａから機器Ｂを認証するものとする。ここで機器Ａは、公開鍵ｋｐを保持しており、機器Ｂは、機器Ａとの間で所定のコンテンツ保護機能を共有しているならば、公開鍵ｋｐに対応する秘密鍵ｋｓを

保持している。機器Ａは乱数Ｒを発生して機器Ｂに送る。機器Ｂは、機器Ａで発生された乱数Ｒを受け取ると、それを秘密鍵ｋｓで暗号化して、その暗号化された乱数（ｋｓ［Ｒ］と表す）を機器Ａに返す。機器Ａでは、公開鍵ｋｐを用いて、ｋｓ［Ｒ］を復号し、復号結果が先に発生した乱数Ｒに等しければ、機器Ｂは正しい相手であると判定する。

【００３８】その後、上記と同じことを機器Ｂから機器Ａに対して行うことで、相互認証を行うことができる。この場合、機器Ｂは公開鍵を保持し、機器Ａは秘密鍵を保持し、機器Ａが機器Ｂにて発生した乱数を秘密鍵で暗号化してそれを機器Ｂで公開鍵を用いて復号し、先に発生した乱数に等しいかを確認する。

【００３９】以上の相互認証（Ｓ１０１）により、ＬＣＭ１及びＰＭ１３の双方にて正当な相手であることが確認されたとき、ＬＣＭ１のメディアＩ／Ｆ部６とＰＭ１３のコントローラ１３０との間でキー交換が行われ、同一の認証鍵（K_{X1}）が共有される。このキー交換は、例えばＤＶＤ－ＲＯＭのコンテンツ暗号化アルゴリズムとして使用されているＣＳＳ（Content Scrambling System）に代表されるランダムチャレンジ・レスポンスを用いた方法により行われる。認証鍵（K_{X1}）は毎回代わる時変キーである。

【００４０】ＬＣＭ１のメディアＩ／Ｆ部６は、秘匿領域１１４に秘匿（記憶）されている自身の識別情報$ＩＤ_{LCM}$を読み出して当該$ＩＤ_{LCM}$を認証鍵（K_{X1}）で暗号化し、その暗号化された$ＩＤ_{LCM}$（$=K_{X1}[ＩＤ_{LCM}]$）をメディアＩ／Ｆ部６からＰＭ１３に送る（ステップＳ１０２）。

【００４１】ＰＭ１３のコントローラ１３０は、ＬＣＭ１側からの$K_{X1}[ＩＤ_{LCM}]$を、先のキー交換で取得した認証鍵（K_{X1}）で復号し、$ＩＤ_{LCM}$を得る（ステップＳ１０３）。次にＰＭ１３のコントローラ１３０は、復号したＬＣＭ１の識別情報$ＩＤ_{LCM}$により公開ＲＯＭ領域１３２内のリボケーションリストＲＬを参照し、当該$ＩＤ_{LCM}$に一致する識別情報が登録されているか否かにより、ＬＣＭ１によるＰＭ１３の利用を無効化するか否かを判定する（ステップＳ１０４）。

【００４２】もし、$ＩＤ_{LCM}$に一致する識別情報がリボケーションリストＲＬに登録されている場合には、コントローラ１３０は該当するＬＣＭ１によるＰＭ１３の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【００４３】これに対し、$ＩＤ_{LCM}$に一致する識別情報がリボケーションリストＲＬに登録されていない場合は、コントローラ１３０は該当するＬＣＭ１によるＰＭ１３の利用が許可されているものと判定し、秘匿領域１３４に秘匿されているメディアキーK_Mを読み出し出力する（ステップＳ１０５）。そしてコントローラ１３０は、ＬＣＭ１のメディアＩ／Ｆ部６との間で（当該ＬＣ

ＭＭ１のメディアＩ／Ｆ部６を介して）キー交換を行い、同一の認証鍵（K_{X2}）を共有した上で、上記読み出したメディアキーK_Mを認証鍵（K_{X2}）で暗号化し、その暗号化されたK_M（＝K_{X2}［K_M］）をＬＣＭ１に送る（ステップＳ１０６）。

【００４４】ＬＣＭ１のメディアＩ／Ｆ部６は、ＰＭ１３側からのK_{X2}［K_M］を、先のキー交換で取得した認証鍵（K_{X2}）で復号し、メディアキーK_Mを得る（ステップＳ１０７）。次にＬＣＭ１のメディアＩ／Ｆ部６は、秘匿領域１１４に秘匿されているコンテンツキーK_Cを取得したメディアキーK_Mにより暗号化し、その暗号化されたK_C（＝K_M［K_C］）をＰＭ１３の公開Ｒ／Ｗ領域１３３に書き込む（ステップＳ１０８）。

【００４５】このように本実施形態では、リボケーションリストＲＬに従って無効化（リボケート）されたならばＰＭ１３から渡されることのない（暗号化された）メディアキーK_Mを、当該ＰＭ１３からＬＣＭ１が受け取って、そのＬＣＭ１の秘匿領域１１４に秘匿されているコンテンツキーK_Cを当該メディアキーK_Mにより暗号化して、ＰＭ１３の公開Ｒ／Ｗ領域１３３に書き込むようにしている。このため、ＬＣＭ１とＰＭ１３との間で認証鍵の交換を行い、その認識鍵を用いてコンテンツキーの暗号化／復号化を行う方法に比べて、リボケーションリストＲＬで指定される無効化対象ＬＣＭ（ＰＭ１３を利用しようとする電子機器）を確実に無効化（排除）できる。なお、ＬＣＭ１の公開Ｒ／Ｗ領域１１３に確保された音楽データ格納部１０に蓄積されている暗号化コンテンツ（K_C［Ｃ］）をＰＭ１３に送る際に、上記取得したK_Mで更に暗号化するようにしても構わない。

【００４６】次に、ＰＭ１３に格納された暗号化コンテンツをＰＤ１２上で復号して再生する場合の動作について、図６の流れ図を参照して説明する。まず、再生の指示が例えばＰＤ１２に対してなされ、且つＰＭ１３がＰＤ１２のメディアＩ／Ｆ部１２ｆに装着された段階で、ＰＤ１２のＣＰＵ１２ａとＰＭ１３のコントローラ１３０との間で（前記ステップＳ１０１と同様の）相互認証が行われる（ステップＳ２０１）。そして、この相互認証（Ｓ２０１）により、ＰＤ１２及びＰＭ１３の双方にて正当な相手であることが確認されたとき、ＰＤ１２のＣＰＵ１２ａとＰＭ１３のコントローラ１３０との間でキー交換が行われ、同一の認証鍵（K_{X3}）が共有される。

【００４７】ＰＤ１２のＣＰＵ１２ａは、秘匿領域１２４に秘匿されている自身の識別情報ID_{PD}を読み出して当該ID_{PD}を認証鍵（K_{X3}）で暗号化し、その暗号化されたID_{PD}（＝K_{X3}［ID_{PD}］）をメディアＩ／Ｆ部１２ｆからＰＭ１３に送る（ステップＳ２０２）。

【００４８】ＰＭ１３のコントローラ１３０は、ＰＤ１２側からのK_{X3}［ID_{PD}］を、先のキー交換で取得した認証鍵（K_{X3}）で復号し、ID_{PD}を得る（ステップＳ２０３）。次にＰＭ１３のコントローラ１３０は、復号したＰＤ１２の識別情報ID_{PD}により公開ＲＯＭ領域１３２内のリボケーションリストＲＬを参照し、当該ID_{PD}に一致する識別情報が登録されているか否かにより、ＰＤ１２によるＰＭ１３の利用を無効化するか否かを判定する（ステップＳ２０４）。

【００４９】もし、ID_{PD}に一致する識別情報がリボケーションリストＲＬに登録されている場合には、コントローラ１３０は該当するＰＤ１２によるＰＭ１３の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【００５０】これに対し、ID_{PD}に一致する識別情報がリボケーションリストＲＬに登録されてない場合は、コントローラ１３０は該当するＰＤ１２によるＰＭ１３の利用が許可されているものと判定し、秘匿領域１３４に秘匿されているメディアキーK_Mを読み出し出力する（ステップＳ２０５）。そしてコントローラ１３０は、ＰＤ１２のＣＰＵ１２ａとの間で（当該ＰＤ１２のメディアＩ／Ｆ部１２ｆを介して）キー交換を行い、同一の認証鍵（K_{X4}）を共有した上で、上記読み出したメディアキーK_Mを認証鍵（K_{X4}）で暗号化し、その暗号化されたK_M（＝K_{X4}［K_M］）をＰＤ１２に送る（ステップＳ２０６）。

【００５１】ＰＤ１２のＣＰＵ１２ａは、ＰＭ１３側からのK_{X4}［K_M］を、先のキー交換で取得した認証鍵（K_{X4}）で復号し、メディアキーK_Mを得る（ステップＳ２０７）。次にＰＤ１２のＣＰＵ１２ａは、ＰＭ１３の公開Ｒ／Ｗ領域１３３に記憶されている暗号化されたコンテンツキーK_C（＝K_M［K_C］）を読み込んで、ステップＳ２０７で取得したメディアキーK_Mにより復号し、その復号されたコンテンツキーK_Cを秘匿領域１２４に書き込んで秘匿化する（ステップＳ２０８）。したがってＰＤ１２では、この復号されたコンテンツキーK_C（と、必要ならば先に復号化したメディアキーK_Mと）を利用して、ＰＭ１３の公開Ｒ／Ｗ領域１３３に記憶されている暗号化コンテンツを復号して再生することが可能となる。

【００５２】このように本実施形態では、リボケーションリストＲＬに従って無効化（リボケート）されたならばＰＭ１３から渡されることのない（暗号化された）メディアキーK_Mを、当該ＰＭ１３からＰＤ１２が受け取って、当該ＰＭ１３の秘匿領域１３４に秘匿されている暗号化コンテンツキー（K_M［K_C］）を、そのメディアキーK_Mにより復号化して、ＰＤ１２の秘匿領域１２４に書き込むようにしている。このため、ＰＤ１２とＰＭ１３との間で認証鍵の交換を行い、その認識鍵を用いて暗号化コンテンツキーの復号化を行うのに比べて、リボケーションリストＲＬで指定される無効化対象ＰＤ（ＰＭ１３を利用しようとする電子機器）を確実に無効化できる。

15

【００５３】なお、以上の実施形態では、ＬＣＭ１とＰＭ１３の間、ＰＤ１２とＰＭ１３の間で、秘匿領域に秘匿されている情報、または秘匿領域に秘匿すべき情報の授受を行う際に、当該情報を認証鍵（K_{Xi}）により暗号化するものとしたが、認証鍵による暗号化は必ずしも必要ではない。但し、コンテンツ保護をより確実なものとするには、認証鍵による暗号化を行うことが好ましい。

【００５４】また、以上の実施形態では、リボケーションリストＲＬが公開ＲＯＭ領域１３２に登録されているものとして説明したが、リボケーションリストＲＬが改ざんされない領域であれば良く、例えば秘匿された特定手続でしかアクセスできない秘匿領域１３４に登録されるようにしても良い。

【００５５】また、以上に述べた実施形態では、各ＰＭ１３（の公開Ｒ／Ｗ領域１３３）に予めリボケーションリストＲＬが登録されているものとして説明したが、これに限るものではない。例えば、コンテンツ毎にリボケーションリストＲＬを付加するようにしてもよい。この場合、システムに共通の秘密キー（以下、マスタキーと称する）K_mを用意し、ＥＭＢにより配信されるコンテンツであれば、当該コンテンツをコンテンツキーK_Cにより暗号化して配信する際に、そのコンテンツキーK_CとリボケーションリストＲＬをまとめてマスタキーK_mにより暗号化して（K_m［K_C＋ＲＬ］と表す）送ればよい。また、ＣＤ（コンパクトディスク）等の記憶媒体に予め記憶されるコンテンツ（暗号化コンテンツ）であれば、そのコンテンツの復号キー、つまりコンテンツキーK_CにリボケーションリストＲＬを付加し、両者をまとめてマスタキーK_mにより暗号化して記憶すればよい。なお、マスタキーK_mはＰＭ１３の秘匿領域１３４に予め格納されているものとする。

【００５６】以下、コンテンツ毎にリボケーションリストＲＬを有する場合の動作を説明する。なお、リボケーションリストＲＬには、バージョン情報が付されているものとする。

【００５７】まず、ＥＭＤから配信された、リボケーションリストＲＬ付きの暗号化された音楽コンテンツをＬＣＭ１のＥＭＤＩ／Ｆ部３で受信して、ＳＭＳ２により音楽データ格納部１０に一時格納した後、その「複製」を「子」コンテンツとして、例えばメディアＩ／Ｆ部６に装着されたＰＭ１３に記録（コピー）するチェックアウト時の動作を例に、図７の流れ図を参照して説明する。

【００５８】この場合、チェックアウトの指示が例えばＬＣＭ１のユーザＩ／Ｆ部１５を介してなされ、且つＰＭ１３がＬＣＭ１のメディアＩ／Ｆ部６に装着された段階で、ＬＣＭ１のメディアＩ／Ｆ部６とＰＭ１３のコントローラ１３０との間で相互認証が行われる（ステップＳ３０１）。

【００５９】この相互認証（Ｓ３０１）により、ＬＣＭ

16

１及びＰＭ１３の双方にて正当な相手であることが確認されると、ＬＣＭ１のメディアＩ／Ｆ部６は、K_m［K_C＋ＲＬ］，K_C［Ｃ］をＰＭ１３の公開Ｒ／Ｗ領域１３３に記憶する（ステップＳ３０２，Ｓ３０３）。このとき、ＬＣＭ１のメディアＩ／Ｆ部６とＰＭ１３のコントローラ１３０との間でキー交換が行われ、同一の認証鍵（K_{X5}）が共有される。

【００６０】ＰＭ１３のコントローラ１３０は、公開Ｒ／Ｗ領域１３３に記憶されているK_m［K_C＋ＲＬ］を、秘匿領域１３４に秘匿されているマスタキーK_mにより復号し、K_C＋ＲＬを得る（ステップＳ３０４）。

【００６１】次にコントローラ１３０は、K_C＋ＲＬからコンテンツキーK_Cに付加されているリボケーションリストＲＬを抽出して、当該ＲＬのバージョン情報と秘匿領域１３４に秘匿されている現リボケーションリストＲＬのバージョン情報とを比較し、抽出したリボケーションリストＲＬの方が新しいバージョン情報である場合に、秘匿領域１３４内の現リボケーションリストＲＬを、抽出したリボケーションリストＲＬに更新する（ステップＳ３０５）。これにより、秘匿領域１３４内のリボケーションリストＲＬが最新のものに更新される。なお、秘匿領域１３４にリボケーションリストＲＬが秘匿されていない場合には、抽出したリボケーションリストＲＬをそのまま秘匿領域１３４に登録する。

【００６２】さて、相互認証（Ｓ３０１）により、ＬＣＭ１及びＰＭ１３の双方にて正当な相手であることが確認された場合、ＬＣＭ１のメディアＩ／Ｆ部６は、秘匿領域１１４に秘匿されている自身の識別情報ID_{LCM}を読み出して当該ID_{LCM}を上記認証鍵（K_{X5}）で暗号化し、その暗号化されたID_{LCM}（＝K_{X5}［ID_{LCM}］）をメディアＩ／Ｆ部６からＰＭ１３に送る（ステップＳ３０６）。

【００６３】ＰＭ１３のコントローラ１３０は、ＬＣＭ１側からのK_{X5}［ID_{LCM}］を、先のキー交換で取得した認証鍵（K_{X5}）で復号し、ID_{LCM}を得る（ステップＳ３０７）。次にＰＭ１３のコントローラ１３０は、ステップＳ３０５でのリボケーションリストＲＬ更新の有無を確認した後、復号したＬＣＭ１の識別情報ID_{LCM}により秘匿領域１３４内の最新のリボケーションリストＲＬを参照し、当該ID_{LCM}に一致する識別情報が登録されているか否かにより、ＬＣＭ１によるＰＭ１３の利用を無効化するか否かを判定する（ステップＳ３０８）。

【００６４】もし、ID_{LCM}に一致する識別情報がリボケーションリストＲＬに登録されている場合には、コントローラ１３０は該当するＬＣＭ１によるＰＭ１３の利用を無効化すべきものと判定し、公開Ｒ／Ｗ領域１３３に記憶されたK_m［K_C＋ＲＬ］，K_C［Ｃ］を消去して（または無効化して）、以降の処理を停止する。

【００６５】これに対し、ID_{LCM}に一致する識別情報

がリボケーションリストＲＬに登録されてない場合は、コントローラ１３０は該当するＬＣＭ１によるＰＭ１３の利用が許可されているものと判定し、キーの受け渡し等、以降の処理を継続する。

【００６６】以上の動作は、ＣＤ（コンパクトディスク）をＬＣＭ１のＣＤＩ／Ｆ部１１に装着して、当該ＣＤに予め記憶されているリボケーションリストＲＬ付きの暗号化された音楽コンテンツをＳＭＳ２により音楽データ格納部１０に一時格納した後、その「複製」を「子」コンテンツとして、例えばメディアＩ／Ｆ部６に装着されたＰＭ１３に記録（コピー）する場合についても同様である。

【００６７】次に、ＰＭ１３（の公開Ｒ／Ｗ領域１３３）に格納された暗号化コンテンツをＰＤ１２上で復号して再生する場合の動作について、図８の流れ図を参照して説明する。まず、再生の指示が例えばＰＤ１２に対してなされ、且つＰＭ１３がＰＤ１２のメディアＩ／Ｆ部１２ｆに装着された段階で、ＰＤ１２のＣＰＵ１２ａとＰＭ１３のコントローラ１３０との間で相互認証が行われる（ステップＳ４０１）。そして、この相互認証（Ｓ４０１）により、ＰＤ１２及びＰＭ１３の双方にて正当な相手であることが確認されたとき、ＰＤ１２のＣＰＵ１２ａとＰＭ１３のコントローラ１３０との間でキー交換が行われ、同一の認証鍵（K_{X6}）が共有される。

【００６８】ＰＤ１２のＣＰＵ１２ａは、秘匿領域１２４に秘匿されている自身の識別情報ID_{PD}を読み出して当該ID_{PD}を認証鍵（K_{X6}）で暗号化し、その暗号化されたID_{PD}（$=K_{X6}[ID_{PD}]$）をメディアＩ／Ｆ部１２ｆからＰＭ１３に送る（ステップＳ４０２）。

【００６９】ＰＭ１３のコントローラ１３０は、ＰＤ１２側からの$K_{X5}[ID_{PD}]$を、先のキー交換で取得した認証鍵（K_{X6}）で復号し、ID_{PD}を得る（ステップＳ４０３）。次にＰＭ１３のコントローラ１３０は、復号したＰＤ１２の識別情報ID_{PD}により秘匿領域１３４内のリボケーションリストＲＬを参照し、当該ID_{PD}に一致する識別情報が登録されているか否かにより、ＰＤ１２によるＰＭ１３の利用を無効化するか否かを判定する（ステップＳ４０４）。

【００７０】もし、ID_{PD}に一致する識別情報がリボケーションリストＲＬに登録されている場合には、コントローラ１３０は該当するＰＤ１２によるＰＭ１３の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【００７１】これに対し、ID_{PD}に一致する識別情報がリボケーションリストＲＬに登録されてない場合は、コントローラ１３０は該当するＰＤ１２によるＰＭ１３の利用が許可されているものと判定し、秘匿領域１３４に秘匿されているマスタキーK_mを読み出し出力する（ステップＳ４０５）。そしてコントローラ１３０は、ＰＤ１２のＣＰＵ１２ａとの間で（当該ＰＤ１２のメディア

Ｉ／Ｆ部１２ｆを介して）キー交換を行い、同一の認証鍵（K_{X7}）を共有した上で、上記読み出したマスタキーK_mを認証鍵（K_{X7}）で暗号化し、その暗号化されたK_m（$=K_{X7}[K_m]$）をＰＤ１２に送る（ステップＳ４０６）。

【００７２】ＰＤ１２のＣＰＵ１２ａは、ＰＭ１３側からの$K_{X7}[K_m]$を、先のキー交換で取得した認証鍵（K_{X7}）で復号し、マスタキーK_mを得る（ステップＳ４０７）。次にＰＤ１２のＣＰＵ１２ａは、ＰＭ１３の公開Ｒ／Ｗ領域１３３に記憶されている$K_m[K_C+RL]$を読み込んで、ステップＳ４０７で取得したマスタキーK_mにより復号し、その復号されたK_C+RLからコンテンツキーK_Cを抽出する（ステップＳ４０８）。なお、復号されたK_C+RLからK_CとＲＬを抽出するには、例えばK_CとＲＬに所定のヘッダ情報を持たせ、当該ヘッダ情報を検出すればよい。

【００７３】そしてＣＰＵ１２ａは、ＰＭ１３の公開Ｒ／Ｗ領域１３３に記憶されている暗号化コンテンツ（$K_C[C]$）を読み込んで、ステップＳ４０８で取得したコンテンツキーK_Cにより復号し、コンテンツＣを得る（ステップＳ４０９）。これによりＰＤ１２でのコンテンツの再生が可能となる。

【００７４】このように本実施形態では、ＥＭＢから配信された、またはＣＤに記録されたコンテンツをＬＣＭ１によりＰＭ１３に記録する際に、当該コンテンツに付加されたリボケーションリストＲＬに応じて秘匿領域１３４内のリボケーションリストＲＬが最新のものとなるように制御している。このため、各ＰＭ１３毎にリボケーションリストＲＬを用意する場合に比べて、最新のリボケーションリストＲＬに従って、ＬＣＭ１によるＰＭ１３の利用を無効化することができる。また、ＰＭ１３に記録された暗号化コンテンツをＰＤ１２上で再生する際には、リボケーションリストＲＬに従って無効化されたならばＰＭ１３から渡されることのない（暗号化された）マスタキーK_mを、当該ＰＭ１３からＰＤ１２が受け取って、$K_m[K_C+RL]$からコンテンツキーK_Cを復号し、そのコンテンツキーK_Cにより$K_C[C]$からコンテンツを復号するようにしたので、無効化対象ＰＤ１２（ＰＭ１３を利用しようとする電子機器）を確実に無効化できる。

【００７５】

【発明の効果】以上詳述したように本発明によれば、リボケーション情報に従って問題のある機器を検出して記憶媒体の利用を無効化すると共に、無効化しない機器の場合には、無効化されたならば利用不可能な記憶媒体に固有の識別情報をコンテンツまたはコンテンツキーの暗号化または復号化に用いさせることができるため、不当な機器による利用を確実に防止できる。

【００７６】また本発明によれば、リボケーション情報をコンテンツに付加して扱う新規なシステムにより、記

19

憶媒体の特定記憶領域に保持されるリボケーション情報を最新なものに更新でき、これにより常に最新のリボケーション情報に従って不当な機器を効果的に無効化できる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るコンテンツ利用管理システムのブロック構成図。

【図２】図１中のＰＤ（記録再生装置）１２のブロック構成図。

【図３】図１中のＰＭ（記憶メディア）１３のブロック構成図。

【図４】ＬＣＭ１、ＰＤ１２の記憶領域構成例を示す図。

【図５】ＬＣＭ１からＰＭ１３へのコンテンツ記録時の動作手順を説明するための図。

【図６】ＰＭ１３に格納された暗号化コンテンツをＰＤ１２上で復号して再生する場合の動作手順を説明するための図。

【図７】コンテンツ毎にリボケーションリストＲＬを有する場合のＬＣＭ１からＰＭ１３へのコンテンツ記録時

20

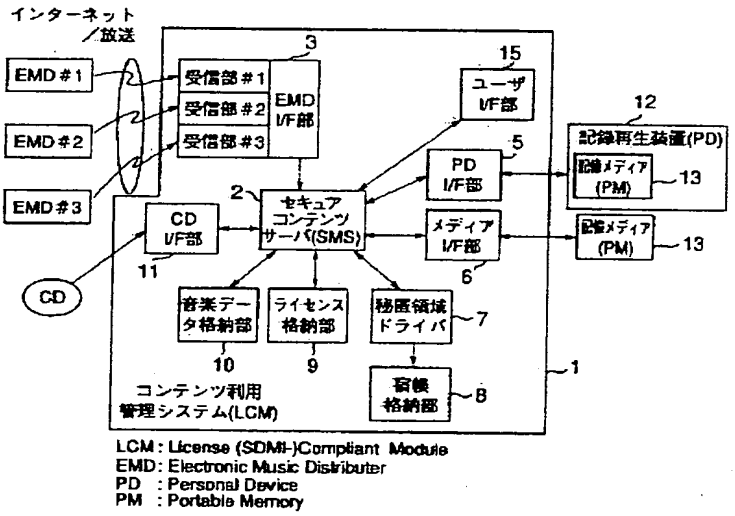
の動作手順を説明するための図。

【図８】コンテンツ毎にリボケーションリストＲＬを有する場合における、ＰＤ１２上でのコンテンツ再生時の動作手順を説明するための図。

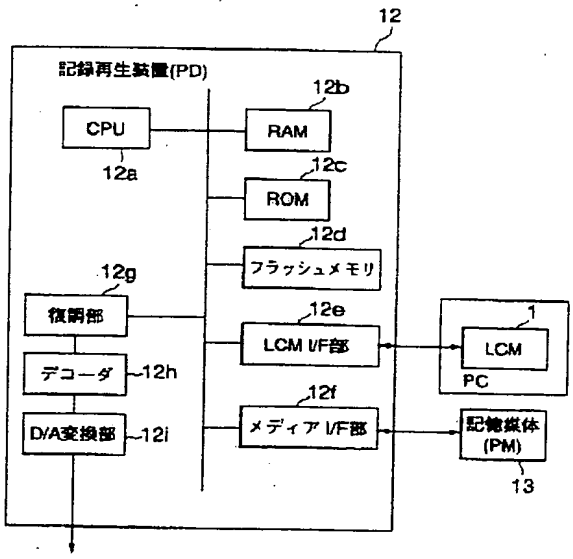
【符号の説明】

１…ＬＣＭ（コンテンツ利用管理システム）
２…ＳＭＳ（セキュア・コンテンツ・サーバ）
５…ＰＤＩ／Ｆ部
６…メディアＩ／Ｆ部
７…秘匿領域ドライバ
８…宿帳格納部
９…ライセンス格納部
１０…音楽データ格納部
１１…ＣＤＩ／Ｆ部
１２…ＰＤ（記録再生装置）
１３…ＰＭ（記憶媒体、記憶メディア）
１１２，１２２，１３２…公開ＲＯＭ領域
１１３，１２３，１３３…公開Ｒ／Ｗ領域
１１４，１２４，１３４…秘匿領域
１３０…コントローラ

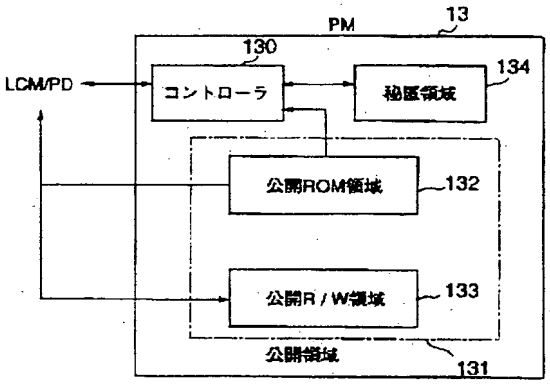
【図１】



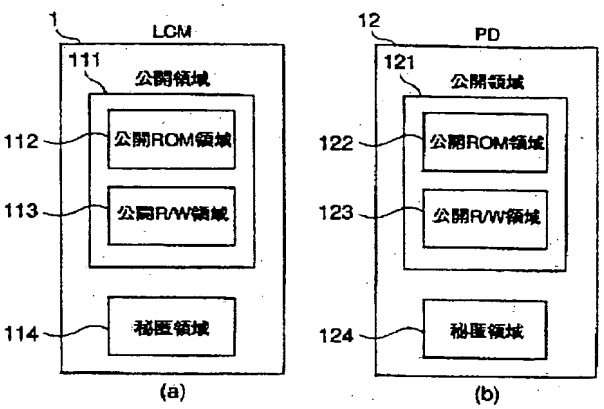
【図２】



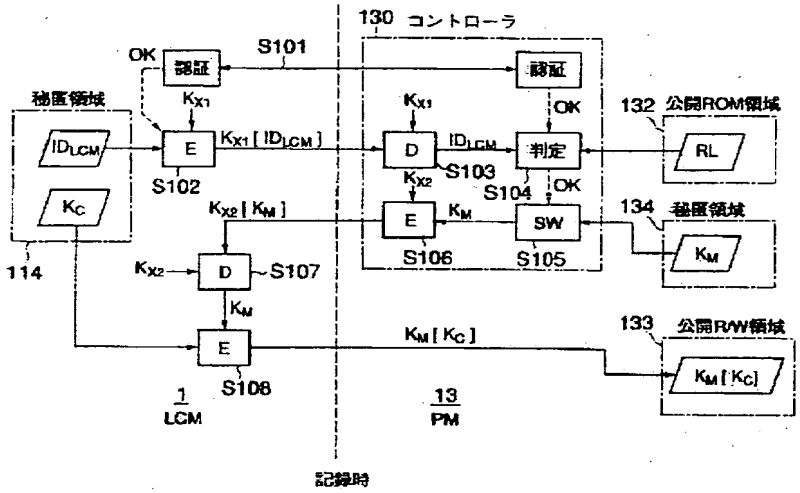
【図３】


PM
13
130
コントローラ
134
秘匿領域
LCM/PD
公開ROM領域
132
公開R/W領域
133
公開領域
131

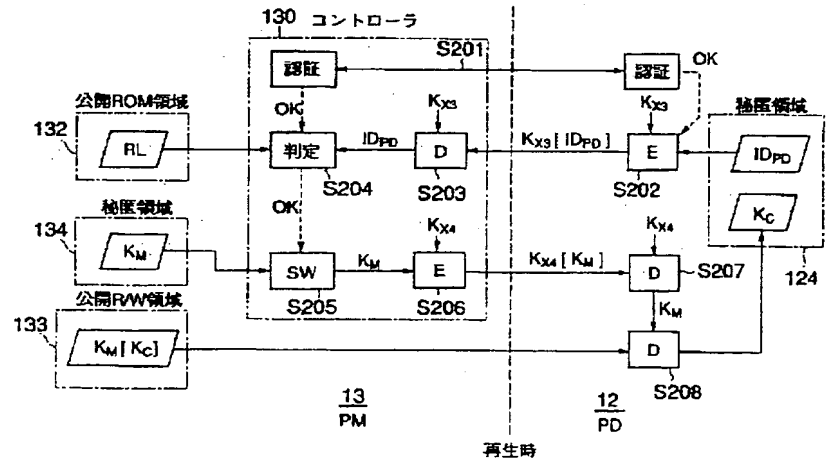
【図４】


1
LCM
111
公開領域
112
公開ROM領域
113
公開R/W領域
114
秘匿領域
(a)
12
PD
121
公開領域
122
公開ROM領域
123
公開R/W領域
124
秘匿領域
(b)

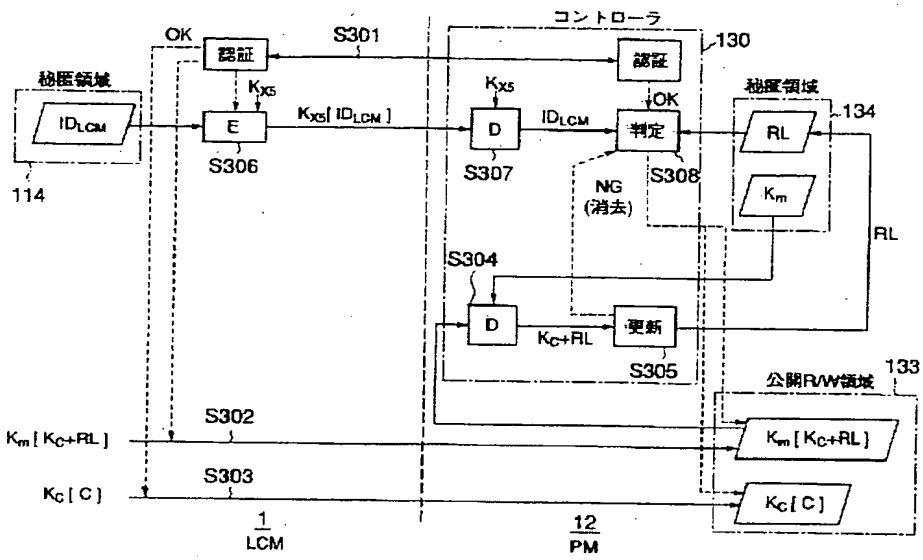
【図５】


130 コントローラ
S101
OK
認証
秘匿領域
K_{X1}
$K_{X1}[ID_{LCM}]$
E
S102
ID_{LCM}
K_C
114
D
判定
S103
S104
K_{X2}
$K_{X2}[K_M]$
K_M
SW
S105
S106
S107
132 公開ROM領域
RL
134 秘匿領域
K_M
133 公開R/W領域
$K_M[K_C]$
S108
1
LCM
13
PM
記録時

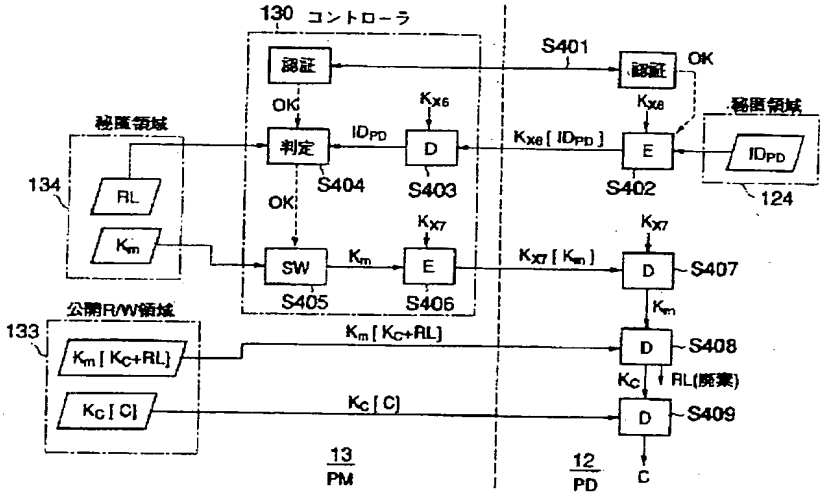
【図６】


130 コントローラ
S201
認証
OK
公開ROM領域
132
RL
判定
ID_{PD}
D
S204
S203
K_{X3}
$K_{X3}[ID_{PD}]$
E
S202
秘匿領域
ID_{PD}
K_C
124
134
K_M
SW
S205
S206
K_{X4}
$K_{X4}[K_M]$
D
S207
公開R/W領域
133
$K_M[K_C]$
S208
13
PM
12
PD
再生時

【図７】



【図８】



フロントページの続き

(72)発明者　岩崎　博
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝マイクロエレクトロニクスセンター内

(72)発明者　田村　正文
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内

(72)発明者　石橋　泰博
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

(72)発明者　加藤　拓
東京都府中市東芝町１番地　株式会社東芝府中工場内

(72)発明者　東間　秀之
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

Ｆターム(参考) 5B017 AA07 BA07 CA15